AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

1. (Cancelled)

2. (Cancelled)

3. (Cancelled)

4 (Cancelled)

5 (Cancelled)

6. (Currently Amended) A method for encrypting and decrypting a message bit string in an information processing system for ~~according to claim 5~~ communicating securely over an insecure communication channel between a pair of correspondents who perform shared key cryptographic operations by implementing respective ones of a pair of complimentary mathematical cryptographic operations utilizing a shared key, said method comprising the steps of:

providing a pair of complimentary mathematical cryptographic operations;

assembling a data string including information to be transferred from a sending correspondent to a receiving correspondent;

performing a complimentary mathematical operation using points on an elliptic curve defined over a finite field and represented in projective coordinates, and wherein an addition of points on the elliptic curve is defined in projective coordinates; and

forwarding the defined group of points over a communication channel to a receiving correspondent and performing the other of the pair of corresponding complimentary mathematical cryptographic operations to decrypt the data; and.

where the elliptic curve points in projective coordinates are represented using three coordinates, (X,Y,Z), wherein X, Y and Z are elements of F(p) represented in N-bit strings, and which includes a step where extra message bits are embedded in the Z coordinate in addition to the message data bits that are embedded in the X coordinate;

embedding a message bit string into the X and Z coordinates of an elliptic curve point which is designated as the message point, $(X_m Y_m Z_m)$;

providing a shared key k and a base point $(X_b Y_b Z_b)$ and computing the scalar multiplication $(X_{bk} Y_{bk} Z_{bk}) = k (X_b Y_b Z_b)$;

computing a cipher point $(X_c Y_c Z_c)$ using $(X_c Y_c Z_c) = (X_m Y_m Z_m) + k(X_b Y_b Z_b)$;

sending appropriate bits of the X-coordinate, X_c and the Z-coordinate Z_c of the cipher point $(X_c Y_c Z_c)$ to a receiving party;

using the shared key k and the base point $(X_b Y_b Z_b)$ computing the scalar multiplication $(X_{bk} Y_{bk} Z_{bk}) = k (X_b Y_b Z_b)$;

computing the message point $(X_m Y_m Z_m)$ using $(X_m Y_m Z_m) = (X_c Y_c Z_c) + (-k (X_b Y_b Z_b))$;

recovering the message bit string from X_m and Z_m;

in which the message bit string is divided into strings of length of M-bit where $(2N-L) > M > (N-L)$;

in which a M-bit message string is further divided into two strings $m_1 m_2$, where the length of string m_1 must be no more than (N-L) bits, while the length of string m_2 must be no more than (N-1) bits; and

which includes the steps of:

assigning the value of the bit string of m_2 to Z_m using the following procedure:

i. assign the value of the bit string m_2 to R_m,
ii. using Legendre test to determine if R_m has a square root,
iii. if R_m has a square root set $Z_m = R_m$ otherwise set $Z_m = gR_m$ where g is any non-quadratic value in the underlying finite filed,

and compute a Z^2_m and bZ^3_m

assign the value of the bit string of m_1 to X_m

compute $T = X^3_m + (aZ^2_m) X_m + (bZ^3_m)$;

using Legendre test to see if T has a square root;

if T has a square root assign one of the roots to Y, if not continue incrementing X_m and repeating the computation of T until T has a square root.

7. (Original) A method for transferring data over a communication channel according to claim 6 in which a second projective coordinate is used by the sending correspondent and to the receiving correspondent to eliminate the inversion or division during each addition and doubling operation of the scalar multiplication.

8. (Original) An encryption and decryption system in accordance with claim 7 and which is implemented either as a pure hardware unit, or as a program stored on a computer readable storage device and executed on a digital computer, or a combination of both.

9. (Cancelled)

10. (Cancelled)

11. (Cancelled)

12 (Cancelled)

13 (Cancelled)

14. (Currently Amended) A method for transferring data over a communication channel between a pair of correspondents who perform public key cryptographic operations by implementing respective ones of a pair of complimentary mathematical operations utilizing a public key and a private key of one of the correspondents, said method comprising the steps of:

providing a data string including information to be transferred from a sending correspondent to a receiving correspondent;

performing a complimentary mathematical operation using a group of points on an elliptic curve defined over a finite field and represented in projective coordinates, and wherein the group of points on the elliptic curve are defined over addition in projective coordinates; and

forwarding the defined group of points over a communication channel to the receiving correspondent and performing the other of the pair of complimentary mathematical cryptographic operations of the public key and the private key cryptographic operation to decrypt the data.~~A method for encrypting and decrypting a message bit string in an information processing system according to claim 13~~

where the elliptic curve points in projective coordinates are represented using three coordinates, (X,Y,Z), wherein X, Y and Z are elements of F(p) represented in N-bit strings, and which includes a step of embedding extra message bits in the Z coordinate in addition to the message data bits that are embedded in the X coordinate; and

including the steps of:

embedding a message bit string into the X and Z coordinates of an elliptic curve point which is designated as the message point, $(X_mY_mZ_m)$ by the sending correspondent;

using the private key of the sending correspondent, k_{SPr}, and the public key of the receiving correspondent, $k_{RPr}(X_bY_bZ_b)$, to compute the scalar multiplication $(X_{bk}Y_{bk}Z_{bk}) = k_{SPr}(k_{RPr}(X_bY_bZ_b))$;

computing a cipher point $(X_cY_cZ_c)$ using $(X_cY_cZ_c) = (X_mY_mZ_m) + (X_{bk}Y_{bk}Z_{bk})$;

sending appropriate bits of the X-coordinate, X_c and the Z-coordinate Z_c of the cipher point $(X_cY_cZ_c)$ to the receiving correspondent;

using the private key of the receiving correspondent, k_{RPr}, and the public key of the sending correspondent, $k_{SPr}(X_bY_bZ_b)$, to compute the scalar multiplication $(X_{bk}Y_{bk}Z_{bk}) = k_{RPr}$

(k_{SPr} ($X_bY_bZ_b$));

computing the message point ($X_mY_mZ_m$) using ($X_mY_mZ_m$) = ($X_cY_cZ_c$) -($X_{bk}Y_{bk}Z_{bk}$);

recovering the message bit string from X_m and Z_m;

in which the message bit string is divided into strings of length of M-bit where (2N-L) > M > (N-L);

in which a M-bit message string is further divided into two strings m_1m_2, where the length of string m_1 must be no more than (N-L) bits, while the length of string m_2 must be no more than (N-1) bits; and

which includes the steps of:

assigning the value of the bit string of m_2 to Z_m using the following procedure:

iv. assign the value of the bit string m_2 to R_m,
v. using Legendre test to determine if R_m has a square root,
vi. if R_m has a square root set $Z_m = R_m$ otherwise set $Z_m = gR_m$ where g is any non-quadratic value in the underlying finite filed,

and compute a Z^2_m and bZ^3_m

assign the value of the bit string of m_1 to X_m

compute $T = X^3_m + (aZ^2_m) X_m + (bZ^3_m)$;

using Legendre test to see if T has a square root;

if T has a square root assign one of the roots to Y, if not continue incrementing X_m and repeating the computation of T until T has a square root.

15. (Original) A method for transferring data over a communication channel according to claim 14 in which a second projective coordinate is used by the sending correspondent and to the receiving correspondent to eliminate the inversion or division during each addition and doubling operation of the scalar multiplication.

16. (Original) An encryption and decryption system in accordance with claim 15 and which is implemented as a pure hardware unit, or as a program stored on a computer readable storage device and executed on a digital computer.

17. (Cancelled)

18. (Cancelled)

19. (Cancelled)

20. (Cancelled)

21. (Cancelled)

22. (Cancelled)